PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-336328
(43)Date of publication of application : 22.12.1995

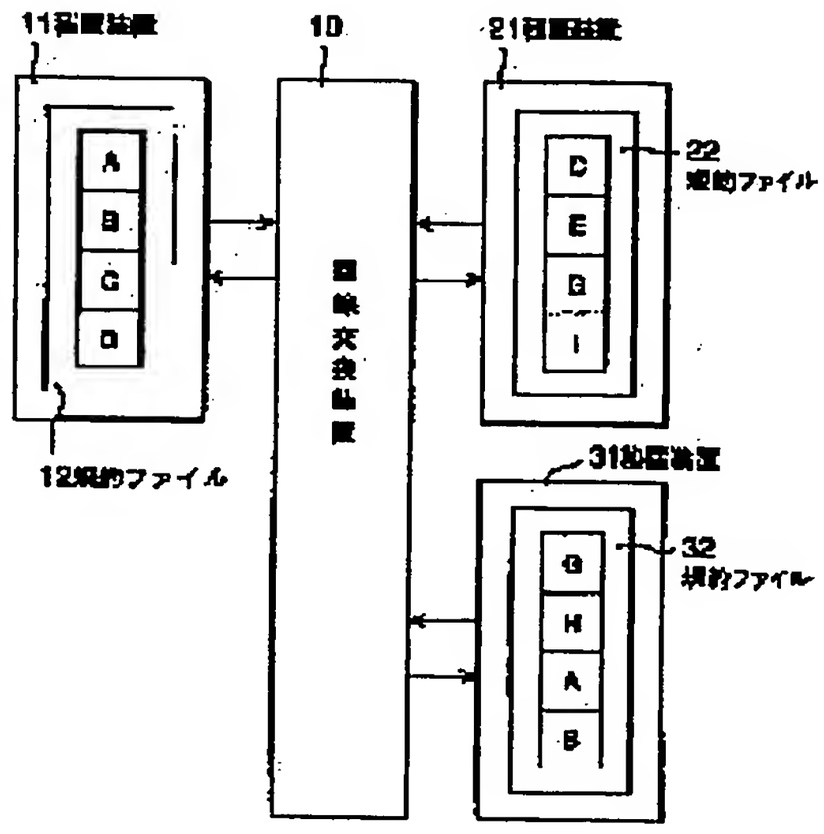
(51)Int.CI. H04K 1/00
G09C 1/00
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : 06-124894
(22)Date of filing : 07.06.1994

(71)Applicant : NEC CORP
(72)Inventor : TAKADA MASA

(54) CIPHER DEVICE

(57)Abstract:
PURPOSE: To make a common cipher system hardly obtain rules even when a cipher device is stolen by selecting the rule held also by a communicating party among the plural rules held by the cipher device by a rule selection means and ciphering and deciphering information data.
CONSTITUTION: In the case of connecting the cipher devices 11 and 21 by a line exchange 10 and performing communication, the device 11 transmits a rule file 12 to the device 21 in its own rule selection part and the rule selection part of the device 21 receives it. Then, the device 11 reports that the rules held by itself are the rules A–D. In the meantime, the device 21 transmits the rule file 22 to the device 11 in its own rule selection part, the rule selection part of the device 11 receives it and it is reported that the rules held by the device 21 are C, E, G and I. The device 11 compares its own rules with the rules of the device 21 in the rule selection part and selects the rule C held by both. In the meantime, comparison is similarly performed in the device 21 as well, the rule C is selected, ciphering and deciphering are performed in a ciphering/–deciphering part by the rule C in the respective devices 11 and 21 and cipher communication between them is performed.



LEGAL STATUS

[Date of request for examination] 07.06.1994
[Date of sending the examiner's decision of rejection] 14.11.1996
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－336328

(43)公開日　平成７年(1995)12月22日

(51)Int.Cl.*		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｋ	1/00	Ｚ			
Ｇ０９Ｃ	1/00		0835－5Ｊ		
Ｈ０４Ｌ	9/00				
	9/10				

Ｈ０４Ｌ　9/00　Ｚ

審査請求　有　請求項の数５　ＯＬ　（全５頁）　最終頁に続く

(21)出願番号　特願平6－124894

(22)出願日　平成６年(1994)６月７日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　高田　雅
東京都港区芝五丁目７番１号　日本電気株式会社内

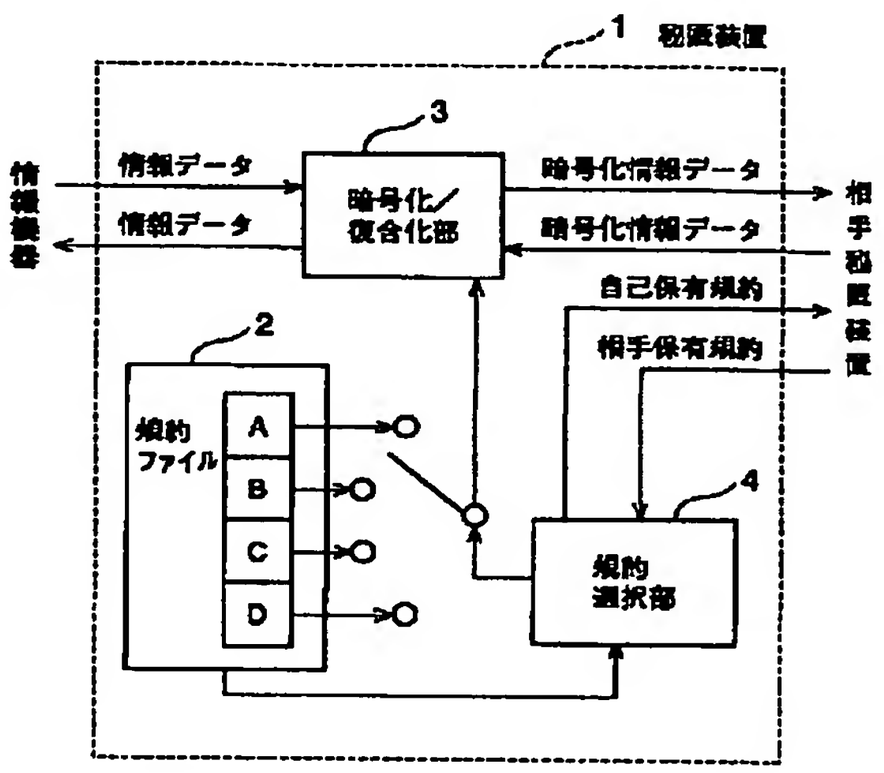
(74)代理人　弁理士　鈴木　弘男

(54)【発明の名称】　秘匿装置

(57)【要約】

【目的】　秘匿装置を第三者に盗まれたとしても、データ通信に用いる慣用暗号系における暗号化鍵および復号化鍵を得にくくすることにより、秘匿性の高い秘匿装置を提供すること。

【構成】　規約選択部４が秘匿装置１が保有する規約ファイル２の複数の規約のうち相手秘匿装置も保有する規約を選択し、この選択した規約で暗号化／復号化部３が情報データの暗号化および復号化を行う。



【特許請求の範囲】
【請求項１】　慣用暗号系の規約で情報データを暗号化および復号化する秘匿装置において、前記暗号化および復号化のための複数の規約を収納する規約ファイルと、該複数の規約のうち通信相手の秘匿装置に合った規約を選択する規約選択手段とを備え、該規約選択手段によって選択された規約で前記情報データの暗号化および復号化を行うようにしたことを特徴とする秘匿装置。
【請求項２】　慣用暗号系の規約で情報データを暗号化および復号化する秘匿装置において、前記暗号化および復号化のための複数の規約を収納する規約ファイルと、該自己の保有する複数の規約を通信相手の秘匿装置に対して送信する自己規約送信手段と、通信相手の保有する複数の規約を通信相手の秘匿装置から受信する相手規約受信手段と、該相手規約受信手段によって受信した通信相手の保有する複数の規約と自己の保有する複数の規約との両方に共通に存在する規約の１つを選択する規約選択手段とを備え、該規約選択手段によって選択された規約で前記情報データの暗号化および復号化を行うようにしたことを特徴とする秘匿装置。
【請求項３】　慣用暗号系の規約で情報データを暗号化および復号化する秘匿装置において、前記暗号化および復号化のための複数の規約を収納する規約ファイルと、該自己の保有する複数の規約を通信相手の秘匿装置に対して送信し、通信相手の保有する複数の規約を通信相手の秘匿装置から受信し、該受信した通信相手の保有する複数の規約と自己の保有する複数の規約の両方に共通に存在する規約の１つを選択する規約選択部とを備え、該規約選択部によって選択された規約で前記情報データの暗号化および復号化を行うようにしたことを特徴とする秘匿装置。
【請求項４】　前記受信した通信相手の保有する複数の規約と自己の保有する複数の規約の両方に共通に存在する規約が複数あるときには、自己が発呼をした場合には自己と通信相手の両方に共通して存在する複数の規約のうちの１を任意に選択して通信相手の秘匿装置に指示し該選択した規約で前記情報データの暗号化および復号化を行い、通信相手の秘匿装置が発呼をした場合には前記両方に共通して存在する複数の規約のうちの１であり通信相手の秘匿装置から指示を受けた規約で前記情報データの暗号化および復号化を行うことを特徴とする請求項２または３に記載の秘匿装置。
【請求項５】　慣用暗号系の規約で情報データを暗号化および復号化する秘匿装置どうしを接続して通信する暗号通信方式において、各秘匿装置のそれぞれが複数の規約を保有し、１の秘匿装置が保有する複数の規約と、該１の秘匿装置と通信する他の秘匿装置が保有する複数の規約には少なくとも１つの同じ規約が存在し、前記１の秘匿装置と前記他の秘匿装置とが該同じ規約で暗号通信を行うことを特徴とする暗号通信方式。

【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は秘匿装置に関し、特に慣用暗号系で情報データを暗号化および復号化する秘匿装置およびこの秘匿装置を用いた暗号通信方式に関する。
【０００２】
【従来の技術】たとえば、銀行預金をオンラインのキャッシュディスペンサ等から引き出すときには、このキャッシュディスペンサ等から預金者の通帳番号や暗証番号を通信回線を介してセンタのホストコンピュータに送信し、預かり残高の確認などが行われるが、このとき、通信回線等から預金者の通帳番号や暗証番号が第三者によって傍受されてしまうなど、個人情報が漏洩し悪用されるおそれがある。
【０００３】そこで、このような重要な情報データを通信する場合には、情報データを暗号化して第三者が傍受しても解読不可能な状態にすることが必要である。つまり、暗号化鍵と復号化鍵とを備えた秘匿装置を送信側および受信側に設け、送信側では暗号化鍵によって情報データを暗号化した上で送信し、受信側では受信した暗号化された情報データを復号化鍵によって元の情報データに復号化する。
【０００４】従来から知られた暗号系としては、慣用暗号系（対称暗号系）と公開鍵暗号系（非対称暗号系）とがある。慣用暗号系とは暗号化鍵と復号化鍵とが同一あるいは復号化鍵が暗号化鍵から容易に生成し得る系をいい、公開鍵暗号系とは一方の鍵から他方の鍵が事実上算出不可能となるように２つの鍵を定める系をいう。
【０００５】慣用暗号系の場合にはどちらかの鍵が第三者に公開されてしまうと暗号化された情報データがその第三者により解読されてしまうという欠点があるが、公開鍵暗号系の場合には一方の鍵が第三者に公開されても暗号化された情報データの第三者による解読は不可能である。
【０００６】しかし、公開鍵暗号系の場合、上記の利点があるものの暗号化および復号化にかなりの時間がかかるため、高速のデータ通信には不向きである。一方、慣用暗号系は暗号化および復号化にそれほど時間がかからない。そこで従来は、日常のデータ通信は慣用暗号系で暗号化して行い、鍵の漏洩に対抗するため慣用暗号系における鍵を定期的に変更することとし、この鍵の変更においては変更後の鍵を公開鍵暗号系で暗号化して配送するようにしていた。このようにすれば、情報データの秘匿性も保たれさらに高速のデータ通信に対応できて望ましい。
【０００７】
【発明が解決しようとする課題】しかし、上述したように、慣用暗号系における暗号化鍵および復号化鍵を公開鍵暗号系により暗号化して配送し、日常のデータ通信で用いる慣用暗号系における暗号化鍵および復号化鍵を定

期的に変更する場合であっても、暗号化および復号化を行う秘匿装置を第三者に盗まれてしまうと、慣用暗号系における暗号化鍵および復号化鍵をその第三者が得てしまい、この暗号化鍵および復号化鍵の定期的な変更の前であれば、第三者によって情報データを解読されてしまうおそれがある。

【０００８】本発明は上記の点にかんがみてなされたもので、秘匿装置を第三者に盗まれたとしても、データ通信に用いる慣用暗号系における暗号化鍵および復号化鍵を得にくくすることにより、秘匿性の高い秘匿装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】本発明は上記の目的を達成するために、慣用暗号系の規約で情報データを暗号化および復号化する秘匿装置において、前記暗号化および復号化のための複数の規約を収納する規約ファイルと、この自己の保有する複数の規約を通信相手の秘匿装置に対して送信する自己規約送信手段と、通信相手の保有する複数の規約を通信相手の秘匿装置から受信する相手規約受信手段と、この相手規約受信手段によって受信した通信相手の保有する複数の規約と自己の保有する複数の規約との両方に共通に存在する規約の１つを選択する規約選択手段とを備え、この規約選択手段によって選択された規約で前記情報データの暗号化および復号化を行うようにしたこと。

【００１０】

【作用】本発明は以上の構成によって、規約選択手段が秘匿装置が保有する複数の規約のうち通信相手も保有する規約を選択し、この選択した規約で暗号化／復号化手段が情報データの暗号化および復号化を行う。

【００１１】

【実施例】以下本発明を図面に基づいて説明する。

【００１２】図１は、本発明による秘匿装置の一実施例のブロック図である。

【００１３】ここでは、暗号化鍵と復号化鍵との組み合わせを規約と呼び、この規約により暗号化または復号化を行うものとする。

【００１４】秘匿装置１は、規約ファイル２と暗号化／復号化部３と規約選択部４とから成り、情報機器から情報データを受け、その情報データを暗号化し暗号化情報データとして通信相手の秘匿装置に対して送信するとともに、通信相手の秘匿装置により暗号化された暗号化情報データを受信し、その暗号化情報データを復号化し情報データとして情報機器に出力する。

【００１５】規約ファイル２は４種類の規約Ａ、Ｂ、Ｃ、Ｄから成り、この４種類の規約のうちのいずれか１つを規約選択部４が選択し、暗号化／復号化部３ではこの選択された規約によって情報データの暗号化および暗号化情報データの復号化が行われる。

【００１６】図２は、図１に示した秘匿装置１を相互に接続し通信する場合の一実施例のブロック図である。

【００１７】秘匿装置１１、２１、３１は、図１に示した秘匿装置１と同じ構造の装置であり、回線交換装置１０を介して相互に接続される。

【００１８】ここで、秘匿装置１１内の規約ファイル１２の規約は規約Ａ、Ｂ、Ｃ、Ｄの４種類であり、秘匿装置２１内の規約ファイルの規約２２は規約Ｃ、Ｅ、Ｇ、Ｉの４種類であり、秘匿装置３１内の規約ファイル３２の規約は規約Ｇ、Ｈ、Ａ、Ｂの４種類である。

【００１９】回線交換装置１０により秘匿装置１１、２１、３１のいずれか２つが相互に接続された場合には、まず、相互に自己が保有する規約の送信が行われる。たとえば、回線交換装置１０により秘匿装置１１と秘匿装置２１とが接続されて通信する場合には、秘匿装置１１は、自己の規約選択部４により規約ファイル１２を秘匿装置２１に対して送信し秘匿装置２１が自己の規約選択部４によりこれを受信して、自己が保有する規約が規約Ａ、Ｂ、Ｃ、Ｄの４種類であることを伝え、一方、秘匿装置２１は、自己の規約選択部４により規約ファイル２２を秘匿装置１１に対して送信し秘匿装置１１が自己の規約選択部４によりこれを受信して、自己が保有する規約が規約Ｃ、Ｅ、Ｇ、Ｉの４種類であることを伝える。

【００２０】そして、秘匿装置１１は、自己の規約選択部４において、自己が保有する規約と秘匿装置２１が保有する規約とを比較し、両者がともに保有する規約を選択する。ここでは、規約Ｃのみを両者がともに保有するので規約Ｃを選択する。一方、秘匿装置２１も、自己の規約選択部４において、自己が保有する規約と秘匿装置１１が保有する規約とを比較し、両者がともに保有する規約を選択する。ここでも、やはり規約Ｃのみを両者がともに保有するので規約Ｃを選択する。

【００２１】秘匿装置１１は、自己の規約選択部４で選択した規約Ｃによって自己の暗号化／復号化部３における暗号化および復号化を行うこととし、一方、秘匿装置２１は、自己の規約選択部４で選択した規約Ｃによって自己の暗号化／復号化部３における暗号化および復号化を行うこととして、秘匿装置１１と秘匿装置２１との規約Ｃによる暗号通信が実現する。

【００２２】上述の秘匿装置１１と秘匿装置２１との通信のように、両者がともに保有する規約が１種類の場合にはその規約を選択すればよいが、秘匿装置１１と秘匿装置３１とが通信する場合のように、両者がともに保有する規約が複数種類（規約ＡおよびＢの２種類を両者がともに保有している）の場合には、たとえば、発呼をした側の秘匿装置が、両者がともに保有する複数種類の規約のうちの１種類を任意に選択して通信相手の秘匿装置に伝え、この選択した規約によって暗号通信を行うようにすればよい。

【００２３】なお、上述した実施例では、１つの秘匿装置が保有する規約の種類を４種類としたが、本発明はこ

れに限らず、１つの秘匿装置が複数種類の規約を保有し、通信相手の秘匿装置と自己とがともに保有する規約が少なくとも１種類あればよい。

【００２４】次に、本発明による秘匿装置の別の実施例を説明する。

【００２５】図３は、本発明による秘匿装置の別の実施例のブロック図である。

【００２６】秘匿装置４１は、規約ファイル４２と暗号化／復号化部４３と規約選択部４４とから成り、情報機器から情報データを受け、その情報データを暗号化し、暗号化情報データとして通信相手の秘匿装置に対して送信するとともに、通信相手の秘匿装置により暗号化された暗号化情報データを受信し、その暗号化情報データを復号化し、情報データとして情報機器に出力する。

【００２７】規約ファイル４２は４種類の規約Ａ、Ｂ、Ｃ、Ｄおよび規約ｘから成り、４種類の規約Ａ、Ｂ、Ｃ、Ｄのうちの１つを規約選択部４が選択し、選択した規約と規約ｘとに基づいて新たな規約を生成し、暗号化／復号化部３ではこの生成された規約によって情報データの暗号化および暗号化情報データの復号化が行われる。この他の点については、図１および図２に示した実施例と同様なので説明は省略する。

【００２８】図３のような構成をとることにより、情報データに対してより解読されにくい暗号化を施すことができるという効果がある。

【００２９】

【発明の効果】以上説明したように、本発明によれば、同一の秘匿装置であっても通信相手によって異なった規約を用いて暗号通信を行うので、秘匿装置を第三者に盗まれたとしても、その時々によって用いる規約が異なり、慣用暗号系における暗号化鍵および復号化鍵を第三者が得にくくすることができる。

【００３０】従って、本発明によれば、秘匿性の高い秘匿装置を提供することができる。

【図面の簡単な説明】

【図１】本発明による秘匿装置の一実施例のブロック図である。

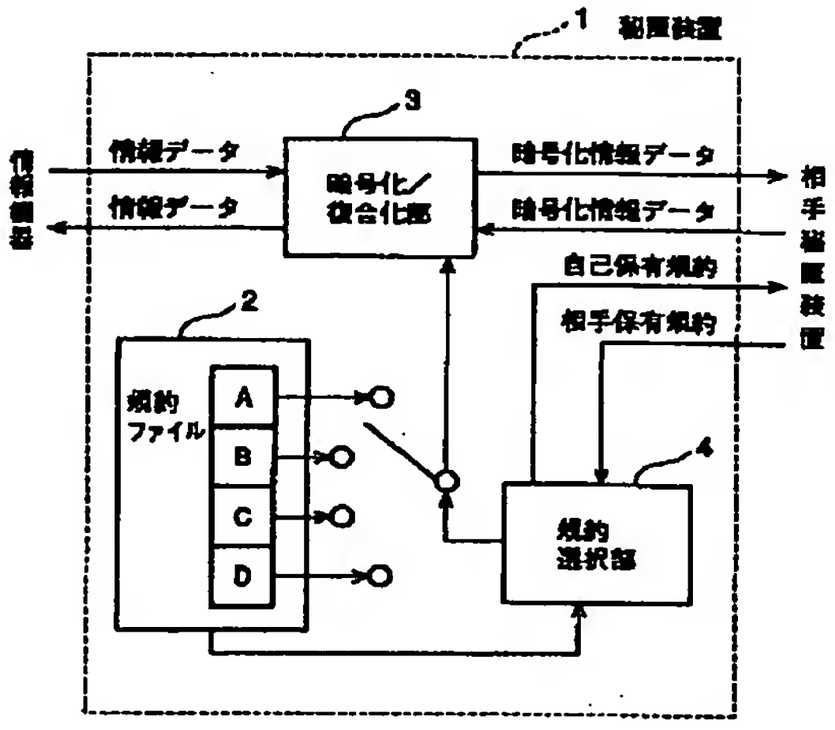
【図２】図１に示した秘匿装置を相互に接続し通信する場合の一実施例のブロック図である。

【図３】本発明による秘匿装置の別の実施例のブロック図である。

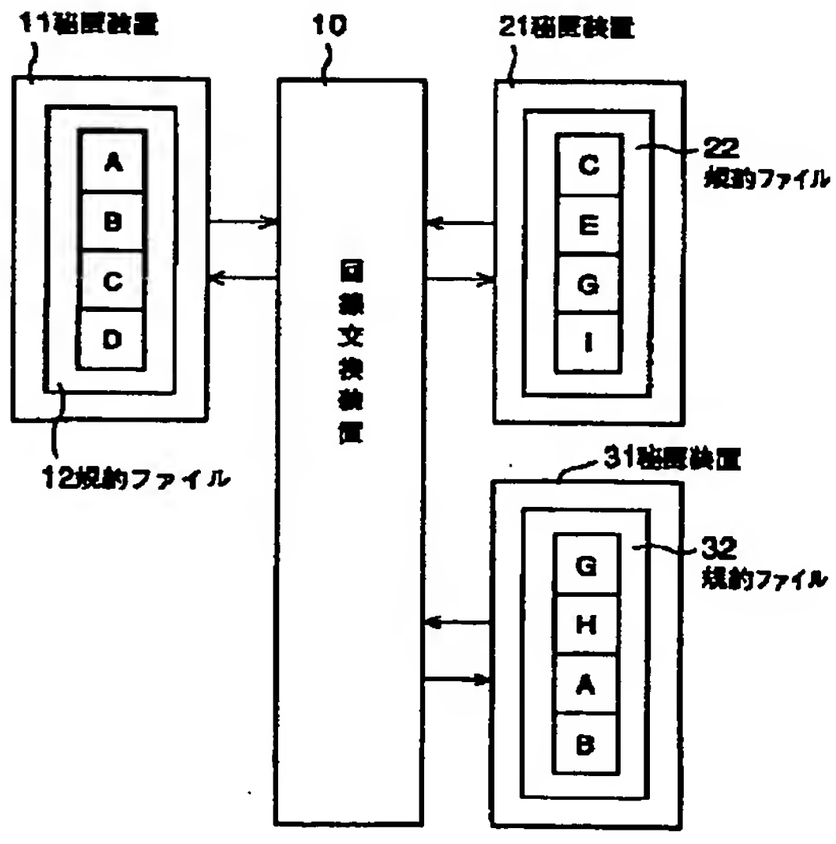
【符号の説明】

１　秘匿装置
２　規約ファイル
３　暗号化／復号化部
４　規約選択部
１０　回線交換装置
１１、２１、３１　秘匿装置
１２、２２、３２　規約ファイル
４１　秘匿装置
４２　規約ファイル
４３　暗号化／復号化部
４４　規約選択部

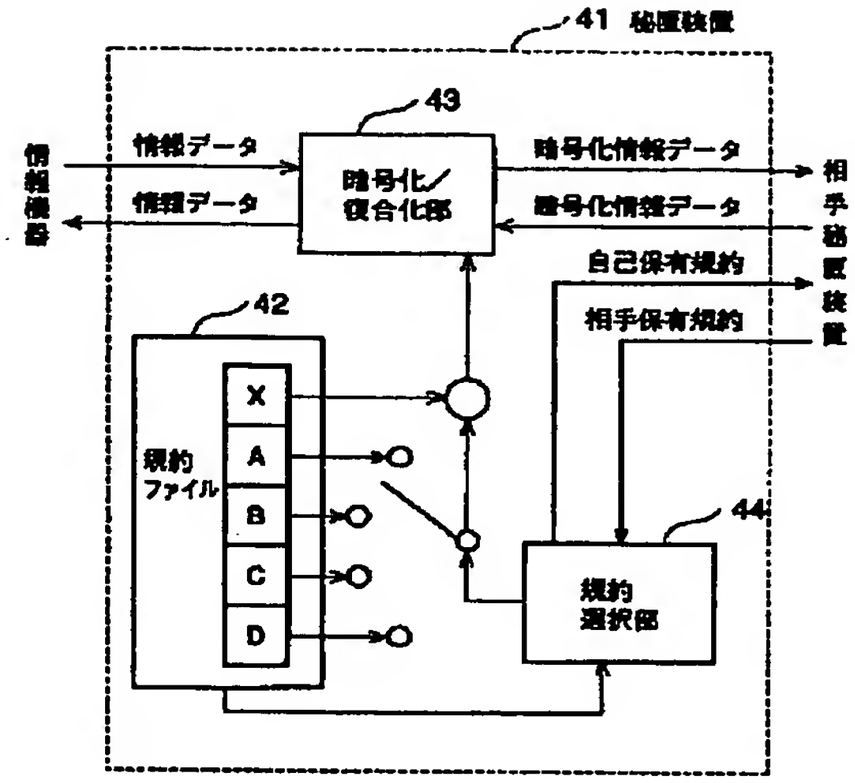
【図１】



【図２】



【図３】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/12				